Symantec™ Gateway Security 300 Series Wireless Implementation Guide

Supported models:

Models 320, 360, and 360R

Symantec™ Gateway Security 300 Series Wireless Implementation Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version 1.0

Part number: 10224358

March 1, 2004

Copyright notice

Copyright © 1998–2004 Symantec Corporation.

All Rights Reserved.

Any technical documentation that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

NO WARRANTY. The technical documentation is being delivered to you AS-IS and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.

No part of this publication may be copied without the express written permission of Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

Trademarks

Symantec, the Symantec logo, and Norton AntiVirus are U.S. registered trademarks of Symantec Corporation. LiveUpdate, LiveUpdate Administration Utility, Symantec AntiVirus, and Symantec Security Response are trademarks of Symantec Corporation.

Other brands and product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Technical support

As part of Symantec Security Response, the Symantec global Technical Support group maintains support centers throughout the world. The Technical Support group's primary role is to respond to specific questions on product feature/function, installation, and configuration, as well as to author content for our Web-accessible Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering as well as Symantec Security Response to provide

Alerting Services and Virus Definition Updates for virus outbreaks and security alerts.

Symantec technical support offerings include:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and Web support components that provide rapid response and up-to-the-minute information
- Upgrade insurance that delivers automatic software upgrade protection
- Content Updates for virus definitions and security signatures that ensure the highest level of protection
- Global support from Symantec Security Response experts, which is available 24 hours a day, 7 days a week worldwide in a variety of languages for those customers enrolled in the Platinum Support program
- Advanced features, such as the Symantec Alerting Service and Technical Account Manager role, offer enhanced response and proactive security support

Please visit our Web site for current information on Support Programs. The specific features available may vary based on the level of support purchased and the specific product that you are using.

Licensing and registration

See "Licensing and regulatory information" on page 37.

Contacting Technical Support

Customers with a current maintenance agreement may contact the Technical Support group by phone or online at www.symantec.com/techsupp/.

Customers with Platinum support agreements may contact Platinum Technical Support by the Platinum Web site at www-secure.symantec.com/platinum/.
When contacting the Technical Support group, please have the following:

- Product release level
- Hardware information
- Available memory, disk space, NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description
- Error messages/log files
- Troubleshooting performed prior to contacting Symantec

- Recent software configuration changes and/or network changes

Customer Service

To contact Enterprise Customer Service online, go to www.symantec.com/techsupp/, select the appropriate Global Site for your country, then select the enterprise Continue link. Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information on product updates and upgrades
- Information on upgrade insurance and maintenance contracts
- Information on Symantec Value License Program
- Advice on Symantec's technical support options
- Nontechnical presales questions
- Missing or defective CD-ROMs or manuals

Contents

Chapter 1 Introduction

Intended audience 7
Accessing the Security Gateway Management Interface 8
Document structure 9
Where to get more information 9
Checking the components list 10

Chapter 2 Planning the wireless network

Physical planning 11
    Extending the access point range 12
    Overlapping access points 12
Client planning 14
    Wireless NICs 14
    VPN client 14

Chapter 3 Installing the wireless card

Preparing to install the wireless card 15
Installing the wireless card 16

Chapter 4 Creating the WLAN

Configuring access points 19
    Preparing to configure the access point 19
    Identifying an access point 20
    Configuring transmission settings 20
    Selecting a radio channel 21
    Disabling the transceiver 22
Configuring roaming settings 22
    Configuring virtual LANs (VLANs) 25
    Example VLAN with port assignments 26
Monitoring wireless status information 29

Chapter 5 Securing the WLAN

Using VPN to secure your wireless network 31
    Configuring a Client-to-Gateway tunnel 31

Configuring Gateway-to-Gateway tunnels 32
Additional WLAN security 33
Encrypting wireless traffic 33
Filtering wireless traffic 34
Securing the beacon 35

Appendix A Licensing and regulatory information

Product certifications 37
SYMANTEC GATEWAY SECURITY APPLIANCE WIRELESS ADD-ON WARRANTY AGREEMENT 38

Appendix B Wireless field descriptions

Basic Settings tab field descriptions 42
Secured WLAN tab field descriptions 43
Status tab field descriptions 44
Advanced tab field descriptions 45

Appendix C About troubleshooting

Accessing troubleshooting information 47

Index

Chapter 1

Introduction

This chapter includes the following topics:

- Intended audience
- Accessing the Security Gateway Management Interface
- Document structure
- Where to get more information
- Checking the components list

All Symantec Gateway Security 300 Series models are wireless capable. They have special wireless firmware and a CardBus slot that can accommodate an optional functional add-on, consisting of an integrated 802.11b/g radio card and antenna, to allow the highest possible integrated security for wireless LANs, when used with clients running the Symantec Client VPN software.

Note: It is very important to enable wireless security for your wireless network. Symantec provides maximum security with its VPN-secured wireless technology, but at minimum, you should enable WEP. Failure to enable wireless security leaves your network at risk for intrusion.

See "Encrypting wireless traffic" on page 33.

Intended audience

This manual is intended for system managers or administrators responsible for installing and maintaining the security gateway. It assumes that readers have a solid base in networking and wireless concepts and experience using the operating systems.

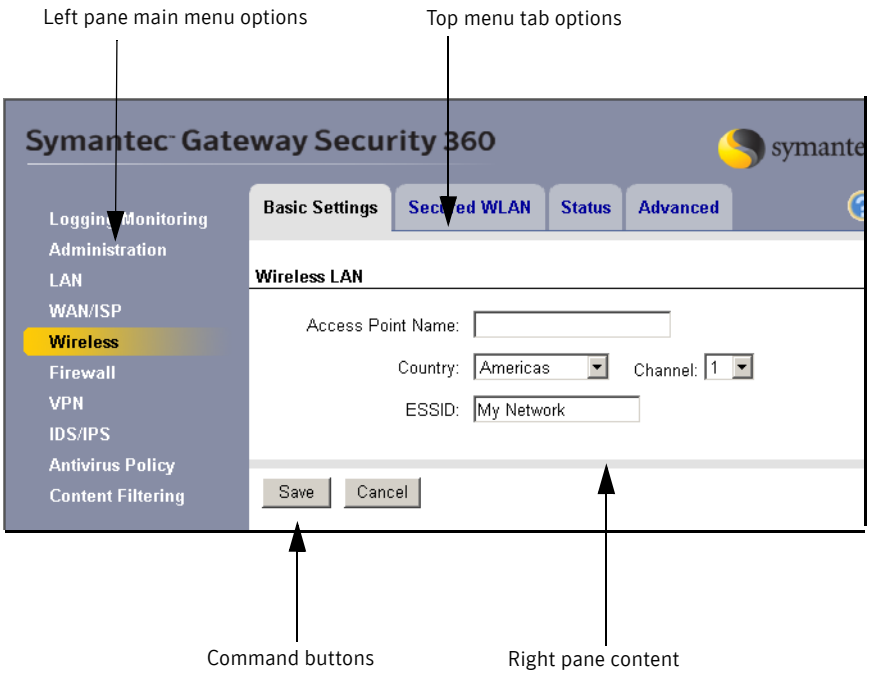
Accessing the Security Gateway Management Interface

You manage the wireless feature through the Security Gateway Management Interface (SGMI). The SGMI is a Web browser-based console where you can create configurations, view status, and access logs. You access the SGMI by browsing to the IP address of the appliance; by default the IP address is 192.168.0.1.

The wireless functionality is only available to configure in the SGMI if the Symantec wireless radio card is installed in the appliance.

Figure 1-1 shows the SGMI when the wireless card is inserted into the appliance.

Figure 1-1 SGMI console with wireless option



For detailed information on using the SGMI, see the *Symantec Gateway Security 300 Series Administrator's Guide.*

Document structure

This manual is structured as follows:

Table 1-1 Document structure

Chapter	Title	Content
Chapter 2	Planning the wireless network	Information to help you plan where to place the appliance if it acts as an access point. Also, information you need to know about how VPN and antivirus policy enforcement work with the wireless feature.
Chapter 3	Installing the wireless card	Instructions for installing the wireless card into the appliance.
Chapter 4	Creating the WLAN	Procedures for configuring the appliance to act as a primary or secondary access point.
Chapter 5	Securing your WLAN with SGMI	Instructions for setting up WEP, VPN, and other configurations that help secure your wireless network.
Appendix A	Licensing	Includes license information for using the wireless radio card with the Symantec Gateway Security 300 Series appliances.
Appendix B	Wireless field descriptions	Descriptions of each field in the user interface that pertains to the wireless functionality.
Appendix C	About troubleshooting	Information for troubleshooting issues and contacting Symantec Technical Support.

Where to get more information

The Symantec Gateway Security 300 Series functionality is described in the following manuals:

- *Symantec™ Gateway Security 300 Series Quick Start Card*
  This card provides abbreviated instructions for installing your appliance.
- *Symantec™ Gateway Security 300 Series Installation Guide*
  This guide covers the physical installation of the appliance, the initial setup of the appliance and the SGMI.

- *Symantec™ Gateway Security 300 Series Administrator's Guide*
  The book describes the Security Gateway Management Interface (SGMI). This guide covers topics related to the appliance and its related components, including: base components, access controls, secure tunnels, VPN policies, remote policies, and monitoring controls. It is provided in PDF format on the Symantec Gateway Security 300 Series Software CD-ROM.

Checking the components list

After carefully unpacking the appliance, compare the actual kit contents with Table 1-2 to ensure that you have received all ordered components.

Table 1-2 Components list

Part	Description
Wireless card	Wrapped in a static-proof bag.
Printed documentation	*Symantec Gateway Security 300 Series Wireless Implementation Guide* *Symantec Gateway Security 300 Series Wireless Release Notes*

Chapter 2

Planning the wireless network

This chapter includes the following topics:

- Physical planning
- Client planning

Physical planning

Like a wired LAN, you must plan for hardware location before setting up the network. The access point is your wireless user's connection to your network and the Internet, so it must be located where the access point and the user's wireless network card can communicate easily.

The location of the access point is crucial for optimal wireless network performance. There are different considerations when doing physical planning for a wireless network. Before you begin installing your wireless network, review the following guidelines regarding placement of the access point:

- Sensitivity and range are inversely proportional to throughput.
  The closer the wireless client is to the access point, the better the data rate. Ensure that you have enough access points close enough together to ensure seamless coverage.
  See "Overlapping access points" on page 12.
- Place the access point as high as you can for best reception.
  The appliance has holes on the bottom of the appliance where you may mount it on a wall.
  See "Extending the access point range" on page 12.

- Place the access point away from clutter.
  Open areas have a better reception range. Physical obstructions like cubicles, metal shelving, or steel pillars can lower performance. Avoid metal barriers.

Extending the access point range

The wireless card by itself can receive a signal from a wireless client. Placing the appliance as high and as far away from clutter helps reception. Attaching a range extending antenna with an MC type connector (such as Orinoco™ IEEE Range Extender) to the wireless card increases and directs the range of the access point. The antenna increases the reception and signal that the access point uses, as well as letting you mount the appliance and point the antenna in the direction where the majority of your wireless users access the appliance. You can extend the access point range before or after installation.

To attach a wireless antenna to the wireless card

1. Turn off the appliance by pressing the power button.
2. Attach the cord from the antenna to the antenna port on the end of the wireless card.
3. Turn on the appliance by pressing the power button.

Overlapping access points

To create an extended WLAN, you use multiple access points, with one acting as a primary and the remainder acting as secondary. You connect the secondary access points to the primary access point with an Ethernet cable from LAN port to LAN port. There is a limit of 15 secondary access points in a WLAN.

See "Configuring access points" on page 19.

When planning your network, ensure that the access points are close enough together to ensure seamless roaming for your clients. Use Table 2-1 to plan the location of your primary and secondary access points.

Table 2-1 Wireless ranges and speeds

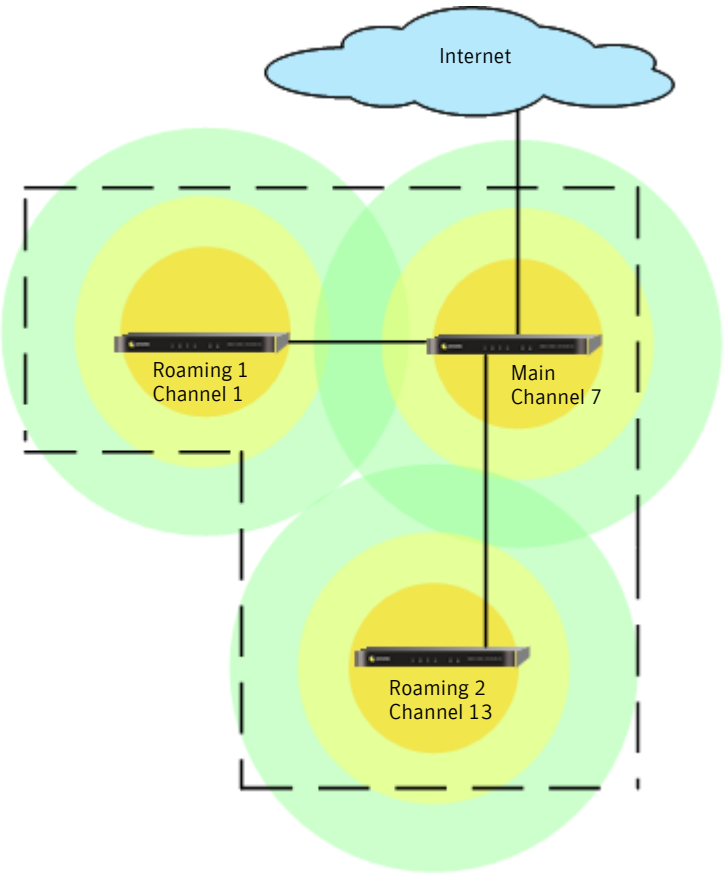
Protocol	Location	Range/Speed
802.11b	Indoors	■ 125 feet (38.1 meters) at 11 Mbps ■ 750 feet (228.6 meters) at 1 Mbps
	Outdoors	■ 450 feet (137.2 meters) at 11 Mbps ■ 1800 feet (548.6 meters) at 1 Mbps

Table 2-1 Wireless ranges and speeds (Continued)

Protocol	Location	Range/Speed
802.11g	Indoors	■ 125 feet (38.1 meters) at 54 Mbps ■ 750 feet (228.6 meters) at 5 Mbps
	Outdoors	■ 450 feet (137.2 meters) at 15 Mbps ■ 1800 feet (548.6 meters) at 1 Mbps

Figure 2-1 shows a primary access point with two secondary access points. Each concentric circle represents decreased reception. Plan to overlap the ranges of your primary and secondary access points. Also plan to assign channel numbers from different parts of the range of available channel numbers to the access points so that the channels do not overlap.

Figure 2-1 Access point range overlap



Client planning

In preparation for clients to connect to your wireless network, you must ensure that they have the proper hardware and software for a successful experience. Also, as administrator, you must configure the appliance for your clients to use antivirus policy enforcement (AVpe) and VPN for secure networks.

Wireless NICs

The appliance's wireless functionality has been tested with and supports the network adapter cards in the following list:

- LinkSys Model WPC55AG Wireless A+G notebook adapter
- US Robotics Model 5410 802.11g wireless turbo card
- 3Com Model sl-1110
- Intel Pro 2011 802.11b
- Netgear Model WG511 802.11b/g 54 Mbps wireless PC card
- Cisco Air 802.11b PCM352 with integrated antenna
- Dlink DWL650 2.4 ghz 802.11b
- LinkSys WPC11 802.11b
- Netgear 802.11b MA701 for PDA
- LinkSys 802.11b WCF11 type II for PDAs
- Hawking CF100w for pocket PC

VPN client

For optimal wireless security, you can require that all wireless LAN users go through a VPN tunnel. If you select this option, each user must have a VPN client, such as Symantec Client VPN.

As the administrator of the appliance, you must also provide each client with the following information for them to enter into the client software:

- IP address of the main gateway (not a roaming IP)
- Shared secret
- If you are using RADIUS authentication, user name (client ID) and password (shared secret). See the *Symantec Gateway Security 300 Series Administrator's Guide* for more information about RADIUS authentication.

Chapter 3

Installing the wireless card

This chapter includes the following topics:

- Preparing to install the wireless card
- Installing the wireless card

Preparing to install the wireless card

Before installing the wireless card, ensure that there is enough area around the appliance to accommodate the wireless card.

Ensure that the location where you place the appliance allows for good communication between the clients and the wireless card as access point.

See "Planning the wireless network" on page 11.

To install the wireless card, you must first turn off the appliance. This disrupts network traffic, so notify your users that traffic will be interrupted, or that you perform these instructions during off hours.

Note: The wireless feature does not appear in the Security Gateway Management Interface (SGMI) until the wireless card provided by Symantec has been properly inserted. Other cards will not work in the appliance.

Installing the wireless card

Figure 3-1 shows the rear panel of model 320 appliances. The wireless card slot is on the side of the appliance, near the reset button (1).

Figure 3-1 Model 320 rear panel

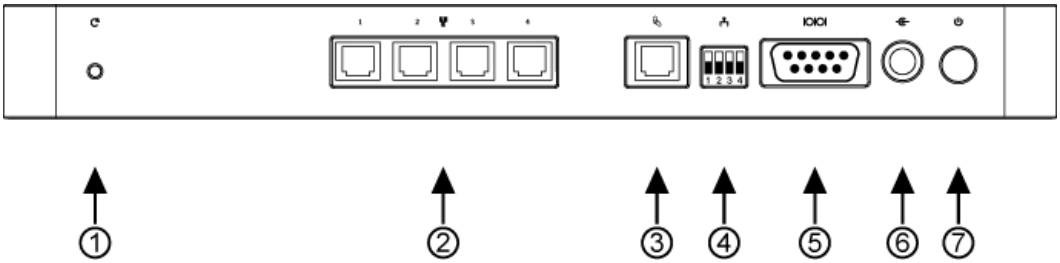
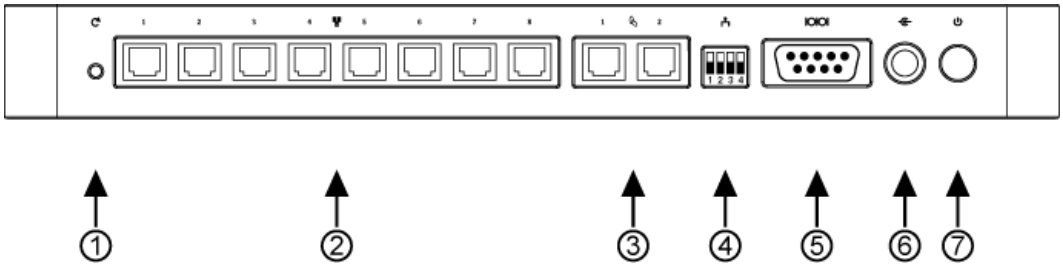


Figure 3-2 shows the rear panel of model 360 and 360R appliances. The wireless card slot is on the side of the appliance, near the reset button (1).

Figure 3-2 Model 360 and 360R rear panel



The numbers in parentheses in the following procedure refer to the rear panel features shown in Figure 3-1 and Figure 3-2.

To install the wireless card

1. Turn off the appliance by pressing the power button (7).
2. Insert the wireless card into the wireless slot (on the right side of the appliance).
3. Turn on the appliance by pressing the power button (7).
4. To begin configuring the wireless feature, browse to the appliance IP address.
   By default, the IP address is 192.168.0.1.

After you have installed the wireless card, you can configure the wireless functionality in the SGMI.

See “Creating the WLAN” on page 19.

It is very important to enable wireless security for your wireless network. Symantec provides maximum security with its VPN-secured wireless technology, but at minimum, you should enable WEP. Failure to enable wireless security leaves your network at risk for intrusion.

See “Encrypting wireless traffic” on page 33.

Installing the wireless card

Chapter 4

Creating the WLAN

This chapter includes the following topics:

- Configuring access points
- Configuring roaming settings
- Monitoring wireless status information

Configuring access points

You can configure Symantec Gateway Security 300 Series appliances to act as wireless access point (AP) devices to provide wireless LAN (WLAN) support with secured 802.11b wireless network routing capability.

Configuring an access point consists of four tasks: preparing to configure the access point, identifying the access point, configuring transmission settings, and selecting a radio channel.

Preparing to configure the access point

Wireless functions are only enabled if the Symantec Gateway Security 300 Series wireless is properly installed.

See "Installing the wireless card" on page 15.

When you install the wireless card, the physical (MAC) address of the appliance in the Logging/Monitoring section changes from the appliance address to the wireless card address.

Identifying an access point

The wireless access point name is unique to the appliance. The access point name gives a unique name to each appliance on the WLAN. Once the connection is made, the access point the client is connected to is reported back to the client. The default access point name is the host name.

The ESSID assigns a unique identifier to a wireless network. When using bridging and roaming, all appliances within the group share the same Extended Service Set Identification number (ESSID). When a client connects to the WLAN, it connects to the ESSID. When you configure roaming within a WLAN, all access points on the wireless network share the same ESSID. Defining an ESSID is a good security practice because it provides a minimal level of security and network segregation. This prevents wireless traffic from different overlapping WLANs from accidentally being shared over the same medium. Creating a unique ESSID also means that only wireless clients that know the ESSID definition can connect to the WLAN.

To identify the access point

See "Basic Settings tab field descriptions" on page 42.

1. In the SGMI, in the left pane, click **Wireless**.
2. To set an access point name, in the right pane, on the Basic Settings tab, in the Access Point Name text box, type a unique name for the appliance.
3. To set the ESSID, in the ESSID text box, type an identifier for the wireless network.
4. Click **Save**.

Configuring transmission settings

The Transmission Settings section is where you set thresholds for wireless traffic to the access point.

See "Advanced tab field descriptions" on page 45.

To configure transmission settings

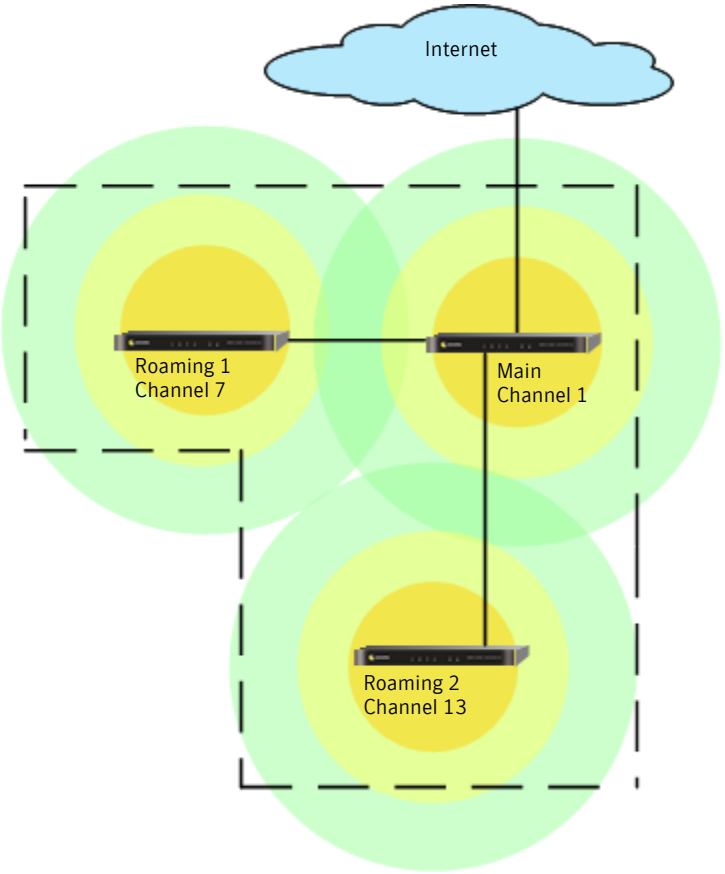
1. In the SGMI, in the left pane, click **Wireless**.
2. In the right pane, on the Advanced tab, under Transmission Settings, in the RTS Threshold text box, type the packet size in bytes.
3. In the Fragment Threshold text box, type the packet size in bytes.
4. Click **Save**.

Selecting a radio channel

Radio frequencies are regulated by different agencies in different countries; therefore, you must select a global region to locate the proper channels that are available in that area. When selecting a specific radio channel to use, select the geographical region and channel number. Each region has different sets of channels.

For optimal performance, if you create a WLAN with multiple access points, set each access point to a channel different from adjacent access points. Figure 4-1 shows different channel settings for adjacent access points in a WLAN. Main is the primary access point; Roaming 1 and Roaming 2 are secondary access points.

Figure 4-1 Channel settings for adjacent access points



To select a radio channel

See "Basic Settings tab field descriptions" on page 42.

1. In the SGMI, in the left pane, click **Wireless**.
2. In the right pane, on the Basic Settings tab, under Wireless LAN, do the following:
   - On the Country drop-down list, select a region.
   - On the Channel drop-down list, select a radio channel.
3. Click **Save**.

Disabling the transceiver

You can disable the transceiver functionality at any time to shut down the wireless functionality without having to remove the card.

To disable the transceiver

See "Advanced tab field descriptions" on page 45.

1. In the SGMI, in the left pane, click **Wireless**.
2. In the right pane, on the Advanced tab, under Transmission Settings, click **Disable Radio**.
3. Click **Save**.

Configuring roaming settings

Roaming lets you extend the physical size of your WLAN by using several Symantec Gateway Security 300 Series appliances to act as a single wireless network. The extended WLAN is composed of several secondary access points and one primary access point (router). You enable roaming on the secondary access points using the Wireless Advanced tab.

There must be a wired connection between the secondary and primary access points. The WAN functionality is disabled on the secondary access points. This configuration provides transparent wireless roaming for all wireless clients on the WLAN.

Note: There is a maximum of 15 secondary access points in a WLAN.

Appliances configured for roaming use the same ESSID to extend the wireless network. The extended wireless coverage areas are called cells. Cells radiate from the appliance in a fairly circular pattern (depending on obstructions).

The DHCP server is disabled automatically on the secondary access point appliances when you enable roaming, since the primary access point in the network is the only one responsible for DHCP services. The secondary access point appliances must use a static IP address on the LAN of primary access point. This IP address must be outside the DHCP range of the primary access point. For each secondary access point, you must configure the appliance as a roaming cell.

Figure 4-2 shows primary and secondary access points and overlapping.

Figure 4-2 Wireless roaming network example

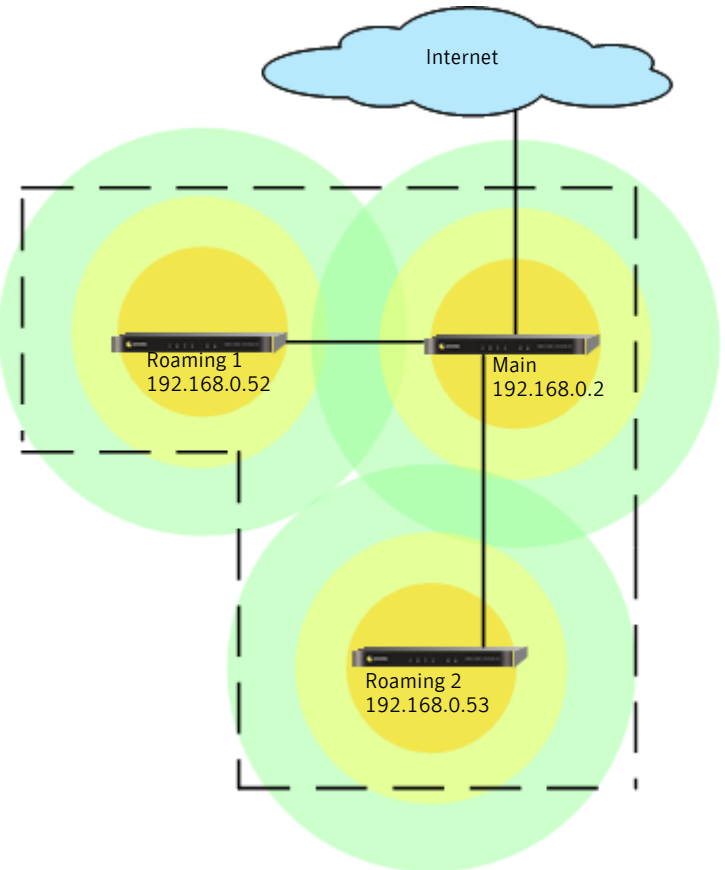


Table 4-1 corresponds to Figure 4-2.

Table 4-1 Wireless roaming network example

	Main (Primary)	Roaming 1 (Secondary)	Roaming 2 (Secondary)
Connection	Wired connection to Internet.	Wired connection to Main from the LAN port.	Wired connection to Main from the LAN port.
DHCP	Range: 192.168.0.2. to 192.168.0.51	Disabled	Disabled
IP Address	192.168.0.2	192.168.0.52 LAN IP is outside the Main DHCP range.	192.168.0.53 LAN IP is outside the Main DHCP range.
Roaming	Disabled	Enabled	Enabled

For best performance, roaming cells should overlap one another so that wireless connectivity in not lost between cells and clients on the LAN.

To configure roaming on secondary access points

Configuring roaming in a wireless network requires two sets of steps. First, you enable roaming, and then you must change the IP address of the appliance.

See the field descriptions in the *Symantec Gateway Security 300 Series Administrator's Guide*.

To enable roaming

1. In the SGMI, in the left pane, click **Wireless**.
2. In the right pane, on the Advanced tab, under Roaming Settings, check **Enable Automatic Roaming**.
3. Click **Save**.

To change the IP address of the appliance

1. In the SGMI, in the left pane, click **LAN**.
2. In the right pane, on the LAN IP & DHCP tab, under LAN IP, type a unique IP address outside the DHCP range of the primary access point, but on the same network.
   For example, if the primary access point has a LAN IP of 192.168.0.1 and a DHCP range of 192.169.0.2 to 192.169.0.51, then each secondary access point should have an IP of 192.169.0.52, 192.169.0.53, 192.169.0.54 and so on.
3. Click **Save**.

Configuring virtual LANs (VLANs)

If you have multiple appliances as access points to create an extended WLAN, to support roaming, you must set each LAN port on each Symantec Gateway Security 300 Series appliance as trusted or untrusted. Secondary access points must connect with an Ethernet cable into a LAN port on the primary access point that is set to SGS Access Point Secured or Enforce VPN/Allow IPsec Pass-thru.

There are three LAN port settings to help you configure your LAN:

- Standard (trusted)
- SGS Access Point Secured (trusted)
- Enforce VPN/Allow IPsec Pass-thru (untrusted)

For information on configuring port settings, see the *Symantec Gateway Security 300 Series Administrator's Guide*.

Standard

When LAN ports are designated as standard, the appliance acts as a typical switch: it forwards traffic based on MAC address and traffic does not reach the security gateway engine unless it was specifically designated for it.

This option does not support client VPN tunnels terminating at the LAN. When a LAN port is set to Standard, it is not considered part of the VLAN.

When you select Standard, VPN traffic is not enforced at the switch, that is, a trusted private network is assumed.

If you choose this option within a wireless network, you should use Wireline Equivalent Protocol (WEP) encryption to secure traffic. You can also configure

the access point to support WEP. For a higher level of security encryption, use VPNs on the WLAN.

See "Encrypting wireless traffic" on page 33.

SGS Access Point Secured

Use this option to set up a secure wireless and wired network that uses Symantec Gateway Security 300 Series appliances as wireless access points.

This option lets wireless clients secure their wireless connection with Symantec Client VPN. They use a global tunnel which terminates at the main appliance, not at the access point. Traffic is reencrypted when it returns to the wireless client.

This option also permits all traffic through the LAN port on the appliance, since the access point is enforcing wireless VPN traffic. No VPN enforcement is done at the LAN port on the appliance.

Enforce VPN/Allow IPsec Pass-thru

Use this option to set up a secure wireless and wired network that uses insecure wireless access points and switches.

This option lets wireless clients use Symantec Client VPN to secure their wireless connections while roaming within the WLAN.

Example VLAN with port assignments

In this example network, Main is a Symantec Gateway Security 300 Series appliance, and is the primary access point. Roaming 1 is another Symantec Gateway Security 300 Series appliance, and is a secondary access point. Roaming 2 is a third-party access point. Roaming 1 has a wired connection to LAN 1 on Main; Roaming 2 has a wired connection to LAN 2 on Main.

To create a virtual LAN, on Main, for Roaming 1, set the port assignment to SGS Access Point Secured. This indicates that it is a trusted connection. For Roaming

2 on Main, set the port assignment to Enforce VPN/Allow IPsec pass-thru. This indicates that it is an untrusted connection.

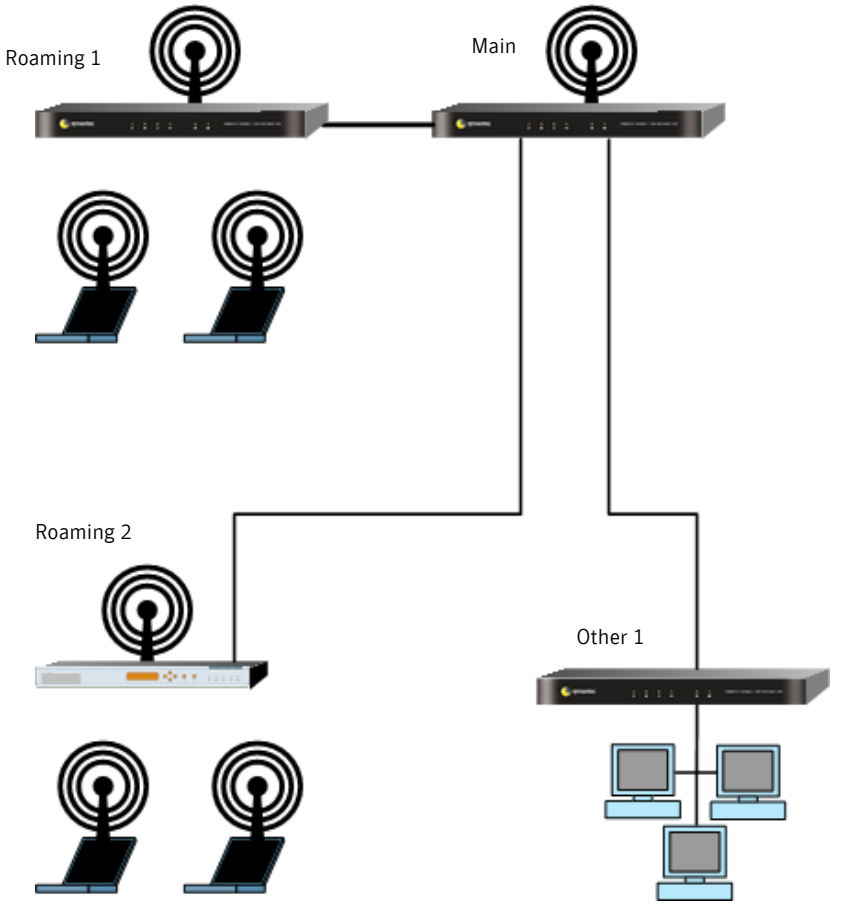
Table 4-2corresponds to Figure 4-3.

Table 4-2 Port assignment examples

Appliance	Port assignment	Description
Main	Differs on each LAN port depending on the appliance that is connected to it.	Symantec Gateway Security 300 Series appliance configured as a primary access point.
Roaming1	SGS Access Point Secured	Symantec Gateway Security 300 Series appliance configured as a secondary access point, connected to Main. Roaming 1 has wireless clients accessing it.
Roaming2	Enforce VPN/Allow IPsec Pass-thru	Third-party security gateway with wireless clients.
Other1	Standard	Symantec Gateway Security 300 Series appliance configured as a security gateway without wireless clients. It is connected to Main.

Figure 4-3 shows a VLAN with appliances that have different port assignments. This figure corresponds to Table 4-2.

Figure 4-3 VLAN with port assignments



Monitoring wireless status information

The Wireless Status information is current when you click view the Status tab. You can refresh the Status window to see if there have been any updates to the Status. It may take up to two minustes to clear status information about wireless that have been disconnected.

To monitor wireless status information

You can view current wireless status, and update it at any time.

See "Status tab field descriptions" on page 44.

To view wireless status information

1. In the SGMI, in the left pane, click **Wireless**.
2. In the right pane, on the Status tab, view the wireless status.

To update the status information

1. In the SGMI, in the left pane, click **Wireless**.
2. In the right pane, on the Status tab, under Receive (Rx) Transmit (Tx), click **Refresh.**

Chapter 5

Securing the WLAN

This chapter includes the following topics:

- Using VPN to secure your wireless network
- Additional WLAN security

Using VPN to secure your wireless network

You can configure a VPN tunnel between the client and the primary access point. This makes the access point like a VPN gateway where the data is secured by a Client-to-Gateway IPsec-like tunnel.

Configuring a Client-to-Gateway tunnel

The primary method for securing your wireless LAN (WLAN) is to ensure that all clients and appliances use VPN tunnels to protect their traffic. When you create a WLAN from several access points, you create Gateway-to-Gateway tunnels between the access points to protect the traffic. For your users to connect to the wireless network, they use Client-to-Gateway tunnels to the primary access point to secure their traffic.

Creating a wireless Client-to-Gateway VPN tunnel that is secured by VPN involves the following steps:

- Define the access point
  See "Configuring access points" on page 19.
- Define and enable remote users
  See *Symantec Gateway Security 300 Series Administrator's Guide*.

- Enable a wireless Client-to-Gateway tunnel
  The following section describes the procedures for enabling a Client-to-Gateway tunnel for wireless use.
- Configure the Client-to-Gateway tunnel
  See *Symantec Gateway Security 300 Series Administrator's Guide*.

Enabling a Client-to-Gateway tunnel to allow wireless clients

Enable the Client-to-Gateway tunnel for wireless clients after you have created and configured the tunnel in the SGMI. See the *Symantec Gateway Security 300 Series Administrator's Guide*.

To enable a Client-to-Gateway tunnel to allow wireless clients

See *Symantec Gateway Security 300 Series Administrator's Guide* for field descriptions.

1. In the SGMI, in the left pane, click **VPN**.
2. On the Client Tunnels tab, under Group Tunnels Definition, in the VPN Group drop-down list, select a VPN group.
3. Check **Enable client VPNs on WLAN/LAN side**.
4. Click **Update**.

Configuring Gateway-to-Gateway tunnels

For optimal security, you should create Gateway-to-Gateway tunnels between your access points. See *Symantec Gateway Security 300 Series Administrator's Guide*.

Symantec Gateway Security 300 Series security gateways support creating a VPN tunnel to up to five remote subnets behind Symantec Enterprise Firewall or Symantec Gateway Security 5400 Series appliances, but not to another Symantec Gateway Security 300 Series appliance or Symantec Firewall/VPN Appliance. Tunnels between two Symantec Gateway Security 300 Series appliances are only made to the subnet on the LAN side of the appliance and only support the first set (subnet/mask) of the five sets of fields, which you define on the VPN > Dynamic Tunnels or VPN > Static Tunnels tabs.

If you have another (additional) subnet on the LAN side of the Symantec Gateway Security 300 Series security gateway, VPN client tunnels to the LAN side of the security gateway are not supported for computers on this separate

subnet. Only computers residing on the appliance subnet (found on the LAN IP screen) are supported for LAN/WLAN-side VPN tunnels.

Note: Gateway-to-Gateway VPN tunnels are supported on the appliance's WAN ports; you cannot define Gateway-to-Gateway VPN tunnels on the appliance's LAN or WLAN ports.

Additional WLAN security

Symantec Gateway Security 300 Series also provides encrypted security for the 802.11b/g wireless link.

You should enable wireless security. Symantec provides maximum security with its VPN secured wireless technology, but at the very least,WEP should be enabled. Failure to enable wireless security leaves your network at risk for intrusion. By combining WEP and requiring VPN on the WLAN, you secure the wireless link.

Encrypting wireless traffic

Symantec Gateway Security 300 Series has encryption options using WEP. You should enable encryption for wireless communication, regardless of whether you are also using VPN. This ensures that only authorized users can wirelessly connect to your network and that all wireless transmissions are encrypted.

There are two levels of WEP encryption: WEP40 (Strong) and WEP104 (Stronger). WEP40 wireless traffic is encrypted with a key length of 5 ASCII characters or 10 HEX characters. WEP104 wireless traffic is encrypted with a key length of 13 ASCII characters or 26 HEX characters. If you enter ASCII characters, after you save the WEP settings, the characters are displayed as HEX for optimal security.

Note: You must have a compatible wireless client (wireless enabled computers that accept Stronger encryption) to use Stronger (WEP104).

To encrypt wireless traffic

See "Secured WLAN tab field descriptions" on page 43.

1 In the SGMI, in the left pane, click **Wireless LAN**.

2 In the right pane, on the Secured WLAN tab, under Wireline Equivalency Protocol (WEP), select an encryption type.

3 In each of the four Key text boxes, type a different key.

4 Click **Save**.

Refer to your wireless client documentation on how to set up WEP on your wireless client and then type the same keys in the same order. If you do not see four key fields in your wireless client configuration, the connection type is not set for access point, sometimes referred to as Enterprise.

Filtering wireless traffic

There are four levels of traffic filtering that let you decide whether to permit VPN traffic on your WLAN, and if so, the parameters for doing so.

- No Enforcement (default)
  The use of VPN on the WLAN is not required. The appliance allows it, but does not require it.
- Enforce VPN Tunnels/Disallow IPsec pass-thru
  When this is enabled, only VPN traffic terminating on the access point is allowed on the WLAN. All other traffic is blocked (except DNS, DHCP, and ARP). This option is used only for primary access points.
- Enforce VPN Tunnels/Allow IPsec pass-thru
  When this is enabled, only VPN traffic terminating on the access point and IPsec pass-thru to other security gateways is allowed on the WLAN. All other traffic is blocked (except DNS, DHCP, and ARP). This option can be used for either primary or secondary access points.
- Allow IPsec pass-thru only
  By default, the access point does not allow IPsec pass-thru to another security gateway. When this is enabled, the appliance allows VPN IPsec traffic destined for another security gateway on the WLAN. All other traffic on the WLAN is blocked (except DNS, DHCP and ARP). Set secondary access points to this option when using VPN-secured wireless. Do not choose this option on a primary access point when using VPN-secured wireless.

To filter wireless traffic

See “Secured WLAN tab field descriptions” on page 43.

1 In the SGMI, in the left pane, click **Wireless**.

2 In the right pane, on the Secured WLAN tab, under Security Settings, in the WLAN VPN drop-down list, select a level of enforcement.

3 Click **Save**.

Securing the beacon

The Extended Service Set Identification (ESSID) is broadcast with the beacon signal. You can additionally secure the WLAN by broadcasting 0 (zero) as the ESSID.

For ease-of-setup, first set up the WLAN clients with the ESSID broadcasting, and then secure the beacon.

Note: Some operating systems, such as Microsoft Windows XP, require the ESSID to be broadcast to join a WLAN.

To secure the beacon

See "Secured WLAN tab field descriptions" on page 43.

1. In the SGMI, in the left pane, click **Wireless**.
2. In the right pane, on the Secured WLAN tab, under Security Settings, check **Hide ESSID**.
3. Click **Save**.

Appendix A

Licensing and regulatory information

This chapter includes the following topics:

- Product certifications
- SYMANTEC GATEWAY SECURITY APPLIANCE WIRELESS ADD-ON WARRANTY AGREEMENT

Product certifications

The following list is product certifications for the Symantec Gateway Security 300 Series 802.11b/g WLAN Access Point Add-on:

- FCC Part 15.401-15.407 & 15.247
- RSS-210, 139-1 (Canada)
- EN 301.893, EN 300.328 (Europe)

A list of countries that are certified to use this product is available on the Symantec Web site.

To view the list of certified countries

1. Browse to www.symantec.com.
2. Click products and services.
3. From the drop-down list, select Symantec Gateway Security 300 Series, and then click **Browse**.

SYMANTEC GATEWAY SECURITY APPLIANCE WIRELESS ADD-ON WARRANTY AGREEMENT

SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO PROVIDE WARRANTIES AS SET FORTH HEREIN ON THE WIRELESS HARDWARE ADD-ON TO BE USED WITH THE APPLIANCE YOU HAVE PURCHASED TO YOU AS AN INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE WIRELESS HARDWARE ADD-ON (REFERENCED BELOW AS "YOU OR YOUR") AND TO PROVIDE WARRANTIES ON THE WIRELESS HARDWARE ADD-ON ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS WARRANTY AGREEMENT. READ THE TERMS AND CONDITIONS OF THIS WARRANTY AGREEMENT CAREFULLY BEFORE USING THE WIRELESS HARDWARE ADD-ON WITH THE APPLIANCE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND SYMANTEC. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING ON THE "AGREE" OR "YES" BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, REQUESTING A LICENSE KEY OR USING THE WIRELESS HARDWARE ADD-ON , YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK ON THE "I DO NOT AGREE" OR "NO" BUTTON IF APPLICABLE AND DO NOT USE THE WIRELESS HARDWARE ADD-ON.

1. Limited Warranty:

Symantec warrants that the wireless hardware add-on component ("Wireless Hardware Add-On) which is to be installed in and used with the appliance You have purchased (the "Appliance") shall be free from defects in material and workmanship under normal use and service and substantially conform to the written documentation accompanying the Wireless Hardware Add-On and/or the Appliance for a period of three hundred sixty-five (365) days from the date of original purchase of the Appliance. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, repair or replace any defective Wireless Hardware Add-On returned to Symantec within the warranty period or refund the money You paid for the Appliance.

The warranties contained in this Agreement will not apply to any Wireless Hardware Add-On which:
A.) has been altered, supplemented, upgraded or modified in any way;
B) has been repaired except by Symantec or its designee; or
C.) has been inserted into, used or operated with any device for which it is not intended as stated in the user documentation accompanying the Wireless Hardware Add-On.

Additionally, the warranties contained in this Agreement do not apply to repair or replacement caused or necessitated by: (i) events occurring after risk of loss passes to You such as loss or damage during shipment; (ii) acts of God including without limitation natural acts such as fire, flood, wind earthquake, lightning or similar disaster; (iii) improper use, environment, installation or electrical supply, improper maintenance, or any other misuse, abuse or mishandling; (iv) governmental actions or inactions; (v) strikes or work stoppages; (vi) Your failure to follow applicable use or operations instructions or manuals; (vii) Your failure to implement, or to allow Symantec or its designee to implement, any corrections or modifications to the Wireless Hardware Add-On made available to You by Symantec; or (viii) such other events outside Symantec's reasonable control.

Upon discovery of any failure of the Wireless Hardware Add-On, or component thereof, to conform to the applicable warranty during the applicable warranty period, You are required to contact us within ten (10) days after such failure and seek a return material authorization ("RMA") number. Symantec will promptly issue the requested RMA as long

as we determine that You meet the conditions for warranty service. The allegedly defective Wireless Hardware Add-On, or component thereof, shall be returned to Symantec, securely and properly packaged, freight and insurance prepaid, with the RMA number prominently displayed on the exterior of the shipment packaging and with the Wireless Hardware Add-On. Symantec will have no obligation to accept any Wireless Hardware Add-On which is returned without an RMA number.

Upon completion of repair or if Symantec decides, in accordance with the warranty, to replace a defective Wireless Hardware Add-On, Symantec will return such repaired or replacement Wireless Hardware Add-On to You, freight and insurance prepaid. In the event that Symantec, in its sole discretion, determines that it is unable to replace or repair the Wireless Hardware Add-On, Symantec will refund to You the F.O.B. price paid by You for the defective Wireless Hardware Add-On. Defective Wireless Hardware Add-Ons returned to Symantec will become the property of Symantec.

Symantec does not warrant that the Wireless Hardware Add-On will meet Your requirements or that operation of the Wireless Hardware Add-On will be uninterrupted or that the Wireless Hardware Add-On will be error-free.

In order to exercise any of the warranty rights contained in this Agreement, You must have available an original sales receipt or bill of sale demonstrating proof of purchase with Your warranty claim.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

2. Disclaimer of Damages:

SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE BELOW LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC OR ITS LICENSORS BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE WIRELESS HARDWARE ADD-ON EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IN NO CASE SHALL SYMANTEC'S OR ITS LICENSORS' LIABILITY EXCEED THE PURCHASE PRICE FOR THE WIRELESS HARDWARE ADD-ON. The disclaimers and limitations set forth above will apply regardless of whether You accept the Wireless Hardware Add-On.

3. Export Regulation:

Certain Symantec products are subject to export controls by the U.S. Department of Commerce (DOC), under the Export Administration Regulations (EAR) (see www.bxa.doc.gov). Violation of U.S. law is strictly prohibited. Licensee agrees to comply with the requirements of the EAR and all applicable international, national, state, regional and local laws, and regulations, including any applicable import and use restrictions. Symantec products are currently prohibited for export or re-export to Cuba, North Korea,

Iran, Iraq, Libya, Syria and Sudan or to any country subject to applicable trade sanctions. Licensee agrees not to export, or re-export, directly or indirectly, any product to any country outlined in the EAR, nor to any person or entity on the DOC Denied Persons, Entities and Unverified Lists, the U.S. Department of State's Debarred List, or on the U.S. Department of Treasury's lists of Specially Designated Nationals, Specially Designated Narcotics Traffickers, or Specially Designated Terrorists. Furthermore, Licensee agrees not to export, or re-export, Symantec products to any military entity not approved under the EAR, or to any other entity for any military purpose, nor will it sell any Symantec product for use in connection with chemical, biological, or nuclear weapons or missiles capable of delivering such weapons.

4. General:

If You are located in North America or Latin America, this Agreement will be governed by the laws of the State of California, United States of America. Otherwise, this Agreement will be governed by the laws of England. This Agreement is the entire agreement between You and Symantec relating to the Wireless Hardware Add-On and: (i) supersedes all prior or contemporaneous oral or written communications, proposals and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment or similar communications between the parties. This Agreement may only be modified by a written document which has been signed by both You and Symantec. This Agreement shall terminate upon Your breach of any term contained herein and You shall cease use of and destroy the Wireless Hardware Add-On. The disclaimers of warranties and damages and limitations on liability shall survive termination. Should You have any questions concerning this Agreement, or if You desire to contact Symantec for any reason, please write: (i) Symantec Customer Service, 555 International Way, Springfield, OR 97477, USA, or (ii) Symantec Customer Service Center, PO BOX 5689, Dublin 15, Ireland.

Appendix B

Wireless field descriptions

This chapter includes the following topics:

- Basic Settings tab field descriptions
- Secured WLAN tab field descriptions
- Status tab field descriptions
- Advanced tab field descriptions

Basic Settings tab field descriptions

The Basic Settings tab lets you define the security gateway as a wireless access point.

Table B-1 Basic Settings field descriptions

Section	Field	Description
Wireless LAN	Access Point Name	Unique name for the security gateway. Identifies the security gateway access point name to wireless clients.
	Country	Region in which the security gateway operates. Each region has its own channel range.
	Channel	Available radio channels. The list of available channels depends on the region you select in the Country drop-down list.
	ESSID	Name for the wireless network. All security gateways on the wireless network use this ESSID. The default ESSID is My Network.The maximum length of the ESSID is 32 alphanumeric characters.

Secured WLAN tab field descriptions

The Secured WLAN tab lets you define the settings for creating a secure wireless network.

Table B-2 Secured WLAN field descriptions

Section	Field	Description
Security Settings	WLAN VPN Secured	Defines how traffic is passed through the security gateway and on to the network. Options include: ■ No Enforcement Allows all wireless traffic to pass. ■ Enforce VPN tunnels/Disallow IPsec pass-thru Requires wireless traffic to use a VPN tunnel terminating on the appliance and does not use IPsec pass-thru. ■ Enforce VPN tunnels/Allow IPsec pass-thru Requires wireless traffic to use a VPN tunnel terminating on the appliance and the traffic can use IPsec pass-thru. ■ Allow IPsec pass-thru only Only allows traffic using IPsec pass-thru (tunnel terminating on external gateway)
	Hide ESSID	By default, the security gateway beacons the ESSID. This lets wireless listeners sniff the ESSID and possibly connect to the WLAN. When ESSID broadcasting is disabled, the client must know the ESSID of the wireless network to connect to the WLAN.

Table B-2 Secured WLAN field descriptions

Section	Field	Description
Wireline Equivalency Protocol (WEP)	Encryption Type	Enables WEP as an encryption method to secure the wireless LAN. Options include: ■ None Wireless traffic is not encrypted. ■ Strong (WEP40) Radio link encryption level of WEP40, wireless traffic is encrypted with a key length of 5 ASCII characters or 10 HEX numbers. ■ Stronger (WEP104) Radio link encryption level of WEP104, wireless traffic is encrypted with a key length of 13 ASCII characters or 26 HEX numbers.
	Key 1, Key 2, Key 3, Key 4	Keys to authenticate wireless clients. In each Key text box, type a different key. ■ If you selected Strong encryption, the key must be 5 ASCII or 10 HEX numbers. ■ If you selected Stronger encryption, the key must be 13 ASCII characters or 26 HEX numbers. Prepend HEX keys with 0x.Remember the keys and the order in which the keys were typed because they must be used in each of the wireless clients.

Status tab field descriptions

The wireless Status tab shows the receive and transmit status of the wireless network. The values that appear in the status fields will vary depending on the amount and nature of the traffic that is passing through the wireless card as well as the clients that are connected to the wireless network.

Table B-3 Receive (Rx)

Section	Status
Receive	Fragments

Table B-3 Receive (Rx)

Section	Status
Transmit	Fragments
Clients Connected	IP Address
	Physical (MAC) Address
	Time Associated

Advanced tab field descriptions

The Advanced tab lets you Transmission Settings section is where you set thresholds for wireless traffic to the access point.

Table B-4 Advanced wireless field descriptions

Section	Field	Description
Transmission Settings	Disable Radio	Turns off the wireless card. This is useful to remotely turn off wireless access without having to physically remove the card from the security gateway.
	RTS Threshold	Request to Send (RTS) sets the packet size (in bytes) that triggers a Request to Send. In congested environments, you may want to make sure that the transmission path is clear by having RTS packets sent before the main packet. The response is a CTS (Clear to Send) and then the Main Packet is sent, otherwise the RTS is repeated. Type 0 (zero) to disable the RTS Threshold.
	Fragment Threshold	Sets the packet size at which you want packets fragmented into smaller packets for more reliable communication in an environment with poor signal quality.
Roaming Settings	Automatic Roaming	Allows clients to roam within the wireless network and disables the DHCP server. Enable this only on secondary access points.

Appendix C

About troubleshooting

You can find up-to-date troubleshooting information for Symantec Gateway Security 300 Series (and all Symantec products) on the Symantec Web site, www.symantec.com.

Accessing troubleshooting information

Use the following procedure to access troubleshooting information from the Symantec Knowledge Base.

To access Symantec Gateway Security 300 Series troubleshooting information

1. Go to www.symantec.com.
2. On the top of the home page, click **support.**
3. Under Product Support > enterprise, click **Continue.**
4. On the Support enterprise page, under Technical Support, click **knowledge base**.
5. Under select a knowledge base, scroll down and click Symantec Gateway Security 300 Series.
6. Click on your specific product name and version.
7. On the knowledge base page for Symantec Gateway Security 300 Series, do any of the following:
   - On the Hot Topics tab, click any of the items in the list to view a detailed list of knowledge base articles on that topic.
   - On the Search tab, in the text box, type a string containing your question. Use the drop-down list to determine how the search is performed and click **Search**.

- On the Browse tab, expand a heading to see knowledge base articles related to that topic.

Index

A

access points 12
    ESSID 20
    maximum secondary access points 22
    naming 20
    radio channel 21
Advanced field descriptions 45
Allow IPsec pass-thru only setting 34, 43
antenna, range extending 12
AVpe clients 14

B

Basic Settings field descriptions 42
beacon settings 35
beacon signal 35
broadcasting, disabling 22, 45

C

cells, overlapping 24
clients 14
Client-to-Gateway tunnels 31
component list 10
components list 10

D

DHCP server 23
documentation, supplied 9

E

Enforce VPN tunnels/Allow IPsec pass-thru setting 34, 43
Enforce VPN tunnels/Disallow IPsec pass-thru setting 34, 43
Enforce VPN/Allow IPsec pass-thru port assignment 26
ESSID 20, 42
    hiding 35, 43
Extended Service Set Identification number. See ESSID
extended WLAN 25

F

field descriptions 41
    Advanced tab 45
    Basic Settings tab 42
    Secured WLAN tab 43
    Status tab 44

G

Gateway-to-Gateway tunnels 32

H

hiding
    ESSID 43
hiding ESSID 35

I

installing, wireless card 15
IPsec 34

L

licensing 37

M

MAC address 19

N

network adapter cards 14
network planning 11
No Enforcement setting 34, 43

O

overlapping access points 12

P

physical address 19
port assignments 25
    Enforce VPN/Allow IPsec Pass-thru 26
    SGS Access Point Secured 26
    Standard 25
product component list 10

R

radio
    disabling 45
radio channels 21, 42
radio, disabling 22
RADIUS authentication 14
range extending antenna 12
regional settings, radio channels 21
roaming 22, 45
    overlapping cells 24

S

secure beacon signal 35
Secured WLAN field descriptions 43
Security Gateway Management Interface (SGMI) 8
SGMI console 8
SGS Access Point Secured port assignment 26
Standard port assignment 25
status 29
Status field descriptions 44
subnet 32
support network adapter cards 14
Symantec Client VPN 14, 26
Symantec Gateway Security 5400 Series 32

T

transceiver, disabling 22, 45
transmission settings, thresholds
    transmission settings 20, 45
troubleshooting 47

U

user documentation 9

V

VPN 27
    clients 14
    Client-to-Gateway tunnels 31
    Gateway-to-Gateway tunnels 32
    subnet 32

W

WEP encryption 33
WEP104 33, 44
WEP128 33, 44
WEP40 33, 44
wireless encryption protocol. *See*WEP
wireless network
    client 14
    physical planning 11
wireless NICs supported 14
wireless status 29
WLAN
     22
    access points 12
    extending 22
    port assignments 25